

# QNAP NAS users, make sure you check your system

---

 [blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/](https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/)

Ma Yanlong

March 5, 2021

5 March 2021 / [QNAP](#)

## Background

---

On March 2, 2021, 360Netlab Threat Detection System started to report attacks targeting the widely used QNAP NAS devices via the unauthorized remote command execution vulnerability (CVE-2020-2506 & CVE-2020-2507)[1], upon successful attack, the attacker will gain root privilege on the device and perform malicious mining activities.

Due to the possible big impact, we contacted and informed the vendor on March 3, and decided to share some information with this quick blog.

Note 1, there is currently no public available PoC for CVE-2020-2506 & CVE-2020-2507, also according to the vendor's request, we are not disclosing the technical details of the vulnerability in order to protect QNAP NAS users, we speculate that there are still hundreds of thousands of online QNAP NAS devices with the vulnerability.

We named the mining program UnityMiner, we noticed the attacker customized the program by hiding the mining process and the real CPU memory resource usage information, so when the QNAP users check the system usage via the WEB management interface, they cannot see the abnormal system behavior.

Previously We have disclosed another QNAP NAS in-the-wild vulnerability attack here[2].

## Vulnerability impact

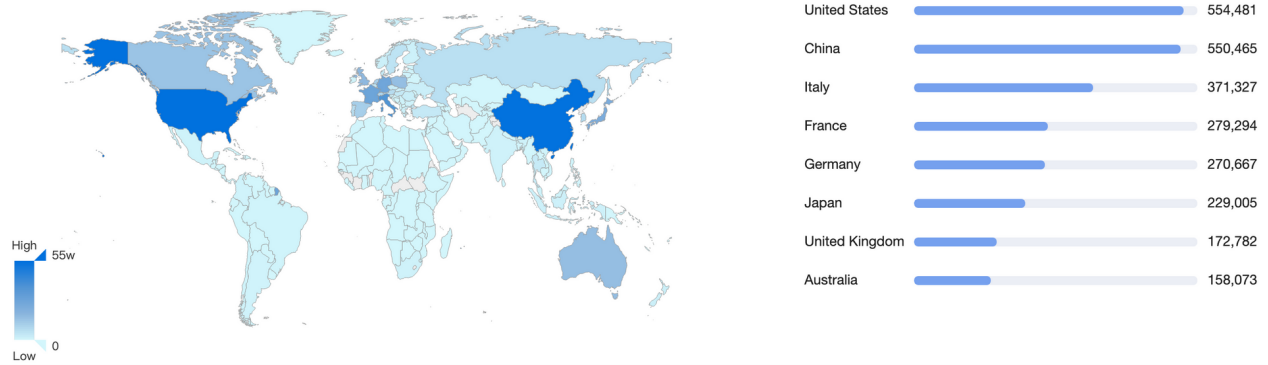
---

Our 360 FirmwareTotal system shows that the following models are affected by the vulnerabilities. The QNAP NAS installed Helpdesk app prior to August 2020 is affected. The following is the list of known models that could be vulnerable.

TVS-X73  
TVS-X71U  
TVS-X71  
TVS-X63  
TS-XA82  
TS-XA73  
TS-XA28A  
TS-X89U  
TS-X88  
TS-X85U  
TS-X85  
TS-X83XU  
TS-X82U  
TS-X82S  
TS-X82  
TS-X80U  
TS-X80  
TS-X77U  
TS-X77  
TS-X73U  
TS-X72U  
TS-X72  
TS-X63U  
TS-X53U  
TS-X53S  
TS-X53D  
TS-X53BU  
TS-X53B  
TS-X53A  
TS-X53  
TS-X51U  
TS-X51DU  
TS-X51B  
TS-X51A  
TS-X51  
TS-X35A  
TS-X28A  
TS-KVM  
TS-879U  
TS-879  
TS-870U  
TS-870  
TS-869U  
TS-869  
TS-859U  
TS-859  
TS-809U  
TS-809  
TS-670  
TS-669  
TS-659  
TS-639  
TS-569  
TS-559  
TS-509

TS-470  
TS-469U  
TS-469  
TS-459U  
TS-459  
TS-439U  
TS-439PROII  
TS-439  
TS-421U  
TS-421  
TS-420U  
TS-420  
TS-419U  
TS-419P  
TS-412U  
TS-412  
TS-410  
TS-269  
TS-259  
TS-239PROII  
TS-239H  
TS-239  
TS-221  
TS-220  
TS-219  
TS-212  
TS-210  
TS-1679U  
TS-1279U  
TS-1270U  
TS-1269U  
TS-121  
TS-120  
TS-119  
TS-112  
TS-110  
TS-1079  
SS-839  
SS-439  
SS-2479U  
SS-1879U  
SS-1279U  
QGD-1600  
Mustang-200  
IS-400  
HS-251  
HS-210

And the following is the Geo breakdown of the devices online by using the 360 Quake cyberspace mapping system, all togetherthere are 4,297,426 QNAP NAS, with 951,486 unique IPs.



## Brief analysis of the mining kit

### 1. Overview

The mining program consists of `unity_install.sh` and `Quick.tar.gz`.

`unity_install.sh` is used to download & set up & start the mining program and hijack the `manaRequest.cgi` program in the original device;

`Quick.tar.gz` contains the miner program, the miner configuration file, the miner startup script and the forged `manaRequest.cgi`.

Unity is the XMRig miner program

```
Quick
├── config.json
├── manaRequest.cgi
├── start.sh
└── unity
```

### 2. `unity_install.sh`

#### Core functions :

- Check if unity process exists, kill if it exists
- Check the CPU architecture of the device and download the mining kit for the corresponding architecture, currently it only supports ARM64 and AMD64
- Set the mining parameters in `config.json` based on the number of CPU cores, the program makes sure it only uses half of the cores for mining.
- Unpack the mining program, set cron and execute the mining script `start.sh` (once every minute, time interval is set directly to `* * * * *`)

### 3. `start.sh`

#### Core function :

- Checking for unity process and starting it if it does not exist.
- Rename the system file `/home/httpd/cgi-bin/management/manaRequest.cgi` to `manaRequests.cgi` (this file is responsible for viewing and modifying the system information of the device)
- Copy the `manaRequest.cgi` file from `Quick.tar.gz` to the `/home/httpd/cgi-bin/management/` directory, replacing the system's own file with the same name.

#### 4. config.json

---

The group uses its own Pool(Proxy), so the real XMR Wallet cannot be seen. There are 3 groups of mining configurations, user are "xmr2", pass are "x", Pool(Proxy) are as follows.

```
aquamangts.tk:12933
a.aquamangts.tk:12933
b.aquamangts.tk:12933
```

#### 5. manaRequest.cgi

---

##### Core function :

Hijack the system's original file of the same name, after receiving HTTP requests, first detect whether there is a unity mining process in the system, if not, then directly transfer the HTTP request to the system's original file of the same name (has been renamed to `manaRequests.cgi` ) to process, and then end the execution of.

```
count=`ps -fe | grep unity | grep -v "grep"`
if [ "" == "$count" ];then
    /home/httpd/cgi-bin/management/manaRequests.cgi
    exit 0
fi
```

If the unity mining process exists on the system, after forwarding the HTTP request to the system's original file of the same name for execution, log the results of the execution (to the `.log.log` file) and then tamper with the execution results by

1. Subtract 50 from the CPU status data
2. Delete the unity process information from the execution result

So when the user suspects something going on with the device and checks the usage, he will see pretty normal CPU usage and tempc, and all the system processes will look normal.

#### Suggestions

---

QNAP NAS users should check and update their firmware promptly.

We recommend that readers monitor and block relevant IPs and URLs mentioned in this blog.

#### Contact us

---

Readers are always welcomed to reach us on [twitter](#), or email to netlab at 360 dot cn.

## IoC

---

### IP:

|                                    |        |         |        |
|------------------------------------|--------|---------|--------|
| 210.201.136.170<br>TECHNOLOGY INC. | Taiwan | ASN9311 | HITRON |
|------------------------------------|--------|---------|--------|

### Miner Proxy:

aquamangts.tk:12933  
a.aquamangts.tk:12933  
b.aquamangts.tk:12933

### URL:

[http://c.aquamangts.tk:8080/QFS/install/unity\\_install.sh](http://c.aquamangts.tk:8080/QFS/install/unity_install.sh)  
<http://c.aquamangts.tk:8080/QFS/arm64/Quick.tar.gz>  
<http://c.aquamangts.tk:8080/QFS/amd64/Quick.tar.gz>

### MD5:

0f40086c9e96c9c11232a9175b26c644  
1eb01a23a122d077540f83b005abdbfc  
97015323b4fd840a40a9d40d2ad4e7af